

FORM PTO-1390
(REV 12-29-99)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

82032-0006

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)

09/763877 ✓

INTERNATIONAL APPLICATION NO.

INTERNATIONAL FILING DATE

PRIORITY DATE CLAIMED

PCT/EP99/06340 ✓

30 August 1999 (30.08.99) ✓

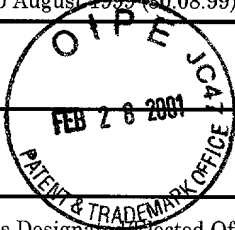
01 September 1998 (01.09.98) ✓

TITLE OF INVENTION:

SECURITY SYSTEM ✓

APPLICANT(S) FOR DO/EO/US

Andrew Augustine WAJS ✓



Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:
 - Courtesy copy of the International Application as published with International Search Report.
 - Courtesy copy of the International Preliminary Examination Report.

U.S. APPLICATION NO. (37 CFR 1.53) **097763877**INTERNATIONAL APPLICATION NO.
PCT/EP99/06340ATTORNEY'S DOCKET NUMBER
82032-0000617. ☒ The following fees are submitted:**BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5):**

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **\$1,000.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO..... **\$860.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO..... **\$710.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy Provisions of PCT Article 33(1)-(4) **\$690.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **\$96.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =**CALCULATIONS PTO USE ONLY**

\$860.00

Surcharge of **\$130.00** for furnishing the oath or declaration later than ☐ 20 X 30 months from the earliest claimed priority date (37 CFR 1.492(e)).

\$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE
Total claims	10-20 =		X \$18.00
Independent claims	1- 3 =		X \$80.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+\$260.00

\$860.00

TOTAL OF ABOVE CALCULATIONS =

Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).

SUBTOTAL =

\$860.00

Processing fee of **\$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).

+

TOTAL NATIONAL FEE =

\$860.00

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **\$40.00** per property

+

TOTAL FEES ENCLOSED =

\$900.00

Amount to be
refunded:

\$

charged:

\$

- a. ☒ A check in the amount of **\$900.00** to cover the above fees is enclosed.
- b. ☐ Please charge my Deposit Account No. _____ in the amount of \$_____ to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1349. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO
HOGAN & HARTSON LLP
Celine Jimenez Crowson
555-13th Street, N.W., 300-W
Washington, D.C. 20004
(202) 637-5703

SIGNATURE:

CELINE JIMENEZ CROWSON
NAME

40.357
REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
)	
Andrew A. WAJS)	371 of International Application
)	
Serial No.: not yet assigned)	IA #: PCT/EP99/06340
)	
Filed: even date herewith)	IA Date: 30 August 99
)	
Title: SECURITY SYSTEM)	
)	ATTY DKT NO.: 82032-00006

PRELIMINARY AMENDMENT

Commisioner of Patents and Trademarks
Washington, D.C.

Sir:

Prior to calculation of the filing fee and examination on the merits,
please amend the above-identified application as follows.

IN THE CLAIMS:

Claim 5, line 1, delete "3 or 4,".

Claim 6, line 2, change "anyone of claims 1-5" to

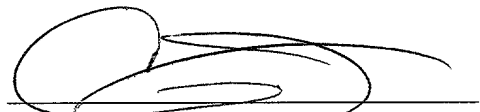
--claim 1--.

Claim 8, line 2, change "anyone of claims 1-5 or for a set of secure
devices (11) according to claim 6 or 7" to --claim 1--.

REMARKS

The above amendments are being made to delete multiple
dependencies in the claims and does not add to or depart from the original
disclosure or constitute prohibited new matter.

Respectfully submitted,



Celine Jimenez Crowson
Attorney for Applicant
Hogan & Hartson, LLP
555 13th Street, N.W., Suite 300-W
Washington, D.C. 20004
PH: 202-637-5600

09/763877

WO 2924-dv/ck

Security system

The present invention relates to a security system for preventing unauthorized use, entrance or the like, comprising a number of secure devices, each of said secure devices comprising a chip with logic circuitry having a
5 function in providing authorization to the security system.

Security systems of the above-mentioned type are used in many applications, such as for example to prevent unauthorized access to secured rooms, in pay tv applications, in banking systems etc. The security devices used are
10 generally made as so-called smart cards comprising a chip. <...> It will be clear that in view of the many smart cards provided to many different persons, security systems of this type are open to attack by pirates or defrauders. Attacking a smart card currently involves a process, wherein during an
15 analysis phase the chip of the smart card is probed to find a means of attack. In this process of attacking the layout of the chip is analysed to identify the appropriate probe points to access the data contained in the chip. Thereafter the attack is planned in a preparation phase and finally the
20 contents of the chip are extracted in the actual attack phase. While the first and second steps typically take months, the third step can be performed in under a day. This means that once a smart card has been cracked for the first time, any second attack is relatively easy. It will be clear
25 that this is a serious problem in security systems. For, once a smart card has been identified as being broken and has been disabled by the controlling system, the pirate can crack another card in a repeated attack within a relatively short period and thereby continue with piracy or fraud.

30 Moreover, the smart cards used in prior art security systems are generally provided with a chip with the same basic silicon layout, even when used in different applications. If for example a smart card of a specific type is
<WO 95/34054 discloses a secure device with a key contained in a separate, hard-wired, circuit.>

hacked for its banking information, the knowledge obtained by hacking this banking card can also be used to extract the secure information from the same type of card when it is used in a different application, for example in a pay television system.

The invention aims to provide a security system of the above-mentioned type wherein the vulnerability for an attack by a pirate is significantly decreased and wherein the time required for a repeated attack of the secure device is substantially increased.

To this end the invention provides a security system of the above-mentioned type, characterized in that in at least a part of said secure devices, the chip of a secure device is provided with a unique chip layout.

In this manner a security system is obtained wherein at least a part but preferably all secure devices are provided with a chip with a random layout of the logic circuitry of the secure device. This means that the hardware implementation of the secure functionality of the secure device varies from device to device.

According to a preferred embodiment at least said logic circuitry of the chips of said part of the secure devices is implemented in FPGA technology, wherein the layout is programmed in the FPGA circuitry either in a volatile or non-volatile manner.

The invention further provides a set of secure devices to be used in a security system of the invention, wherein each of said secure devices comprises a chip with logic circuitry having a function in providing authorization to the holder of a secure device, wherein in at least a part of said secure devices, the chip of each secure device is provided with a unique chip layout.

Finally, the invention provides a method for manufacturing a secure device for the the security system of the invention, wherein secure devices with a chip are used, said chips having logic circuitry having a function in providing authorization to the security system, wherein in

at least a part of said secure devices the chip of a secure device is provided with a unique chip layout.

The invention will be further explained by reference to the drawings, in which an embodiment of the system and
5 method of the invention are schematically shown.

Fig. 1 schematically shows a pay tv system comprising an embodiment of a security system of the invention.

Fig. 2 schematically shows the internal structure of a smart card used as secure device in the system of fig.

10 1.

Fig. 3 shows a diagram of an embodiment of the method of the invention.

Fig. 1 shows merely by way of example a broadcasting system wherein three broadcasters 1-3 are coupled with
15 a multiplexer unit 4. The multiplexer unit 4 comprises means for scrambling, encoding and compressing broadcast signals provided by the broadcasters 1-3 and the thus obtained digital data streams are multiplexed into a digital transport stream. In the embodiment shown this digital transport
20 stream is modulated by way of modulator 5 before transmission. The operator of the equipment including the multiplexer unit 4 and modulator 5 is responsible for transmitting the signal to the receiving equipment of the public, one television set 6 being shown by way of example in fig. 1. One or
25 more of the broadcasters 1-3 may be private broadcasters operating according to the concept of pay tv which implies subscription. This means that people wishing to view programs broadcasted by a particular broadcaster, have to subscribe to such a broadcast and pay the appropriate fee.

30 As schematically indicated the transmission of the signal may be carried out through one or more telecommunication channels including a satellite link 7, terrestrial link 8 or a cable system 9.

Access to anyone of the broadcast signals provided
35 by the broadcasters 1-3 requires a decoder 10 generally including a conditional access module not shown cooperating with a smart card 11 in a manner known per se. The smart

card 11 is one of the secure devices of a security system implemented in the broadcasting system shown in fig. 1 to prevent unauthorized access to pay tv signals by persons which did not subscribe to the broadcast. Each subscriber is
5 provided with a smart card 11, each smart card 11 having a unique key and/or address. This security system may operate for example in a manner known per se using ECM's and EMM's to provide access to the pay tv signals to authorized persons having a smart card 11 with means for providing
10 authorization to the security system.

As explained above, such a security system is open to attack by pirates trying to copy an original smart card to thereby provide a large number of pirate smart cards. In order to substantially increase the time required for a
15 repeated attack on a smart card, the security system described is provided with secure devices or smart cards 11, each of the smart cards comprising a chip with logic circuitry having a function in providing authorization to the system in a conventional manner. The logic circuitry may include
20 the circuitry to store a unique key, and/or the algorithms and logic required to provide authorization, for example the algorithm to decrypt the key hierarchy used in a security system such as eurocrypt.

Fig. 2 shows in a very schematic manner the internal structure of a smart card 11 showing that the chip of the smart card 11 includes a central processing unit 12, an EEPROM circuit 13, a RAM circuit 14 a secure cell 15 and random bus and logic circuitry 16. In the embodiment described the unique circuit layout is provided only in the secure
25 cell 15, in which for example a cryptographic engine and a volatile storage element for storing a secret key are located. For a further explanation of this structure of a smart card reference is made to European Patent Application 97202854.2 of the same applicant.

35 According to a preferred embodiment the secure cell is implemented in FPGA technology (field programmable gate array). The FPGA circuit of the secure cell 15 is program-

med in a usual manner in accordance with the diagram of fig. 3 to personalize the smart card. In order to personalize a smart card 11, unique information is stored in the secure cell, this unique information comprising a unique key, a key decryption algorithm used in the security system or the like. Usually an FPGA is programmed as follows. First the unique information for personalization is written in a high level language, for example C or VHDL. The high level language is first compiled. Thereafter the information is put through a synthesis tool which generates a logic implementation of the high level language code. This logic implementation would generally include logic circuitry such as AND gates, OR gates, D latches etc., which are combined to produce the correct cryptographic functionality. Thereafter the logic implementation is put through a routing program which constructs the actual program file for a particular FPGA. This file will specify which cells are interconnected within the FPGA and how each cell is programmed. The actual program file is then loaded into the FPGA circuit on power up or fuse blown into the FPGA depending on the particular FPGA technology used.

Generally a synthesis tool can produce many variations of the same functionality. In prior art applications the synthesis tool is designed to produce logic which utilizes the minimum number of gates, shows an optimal power efficiency, has the best speed performance or a compromise of the above.

According to the present invention a variation factor¹⁹ for example a random number, is introduced into the synthesis tool²⁰ such that the layout provided by the synthesis tool²⁰ will vary from chip to chip. As schematically shown in the diagram of fig. 3, a variation factor¹⁹ such as a random number is fed into the synthesis tool²⁰ and this results in the tool generating a set of logic which is unique to that variation factor. A new variation factor is used for personalizing each of the smart cards 11 of the security system. In this manner it is obtained that each

6

smart card 11 of the security system has a unique layout of the logic circuitry of the secure cell 15.

Similarly a variation factor²¹ can be fed into the layout tool²² resulting in a further randomizing of the layout
5 of the logic circuitry.

Further it is possible to introduce a variation factor¹⁷ in the compilation step, so that the input to the synthesis tool²⁰ will receive a varying input. All possible variations can be used either separately or in combination.

10 Using the method of the invention the personalization step introducing a unique key, the logic implementation of the key and/or the decryption functions into the smart card 11, will result in a layout of the logic circuitry which is unique to each smart card 11. In this manner it is
15 obtained that the time needed for each attack of a security system is substantially increased as the pirate can not use the information obtained in an analysis phase and a preparation phase in an attack of a first smart card, in attacking another smart card.

20 As an alternative, instead of using FPGA technology in the secure cell only, more parts of the chip or the entire chip of the smart card can be built using FPGA techniques and can then be randomized in the above described manner.

25 In a preferred embodiment a volatile FPGA is used, wherein the FPGA program is stored in RAM 14 of the smart card 11, which is powered by a battery just as the volatile storage of the key in the secure cell 15. Including defense traps as known per se in the smart card chip will result in
30 a loss of the contents of the RAM memory and the volatile storage of the secure cell 15 if a pirate fails to overcome the defense strategy of the chip. Thereby the programming of the FPGA circuitry will be lost. In this manner it is obtained that by attacking a card no information is gathered
35 on how to attack a next card.

Although the invention is explained in the above by reference to a pay tv system, the security system of the

invention can be used in any security system using secure devices¹¹ for providing authority to the holder of the secure device¹¹, such as security systems used to protect rooms, buildings, or the like against unauthorized entrance,
5 banking cards etc. Further, although it is preferred to provide each smart card¹¹ with a unique layout it is also possible to provide groups of cards with a unique layout.

The invention is therefore not restricted to the above described embodiment which can be varied in a number
10 of ways within the scope of the claims.

CLAIMS

1. Security system for preventing unauthorized use, entrance or the like, comprising a number of secure devices⁽¹¹⁾, each of said secure devices⁽¹¹⁾ comprising a chip with logic circuitry^(1b) having a function in providing authorization to the security system, characterized in that in at least a ~~part~~^{groups} of said secure devices⁽¹¹⁾, the chip of a secure device⁽¹¹⁾ is provided with a unique chip layout.

2. Security system according to claim 1, wherein at least said logic circuitry^(1b) of the chips of said part of the secure devices⁽¹¹⁾ is implemented in FPGA technology, wherein the layout is programmed in the FPGA circuitry either in a volatile or non-volatile manner.

3. Security system according to claim 2, wherein the logic circuitry of each secure device chip is provided in a secure cell⁽¹⁵⁾ of the chip.

4. Security system according to claim 1, wherein the complete secure device chip is implemented in FPGA technology, wherein the layout is programmed in the chip either in a volatile or non-volatile manner.

5. Security system according to claim 2, 3 or 4, wherein the logic circuitry or the entire chip is made as a volatile programmable FPGA, wherein the FPGA program is stored in a battery powered RAM.

6. A set of secure devices⁽¹¹⁾ ~~to be used in~~^{for} a security system according to anyone of claims 1-5, wherein each of said secure devices⁽¹¹⁾ comprises a chip with logic circuitry having a function in providing authorization to the holder of a secure device⁽¹¹⁾, wherein in at least a ~~part~~^{groups} of said secure devices⁽¹¹⁾, the chip of each secure device is provided with a unique chip layout.

7. A set according to claim 6, wherein at least said logic circuitry of the chips of said part of the secure devices⁽¹¹⁾ is implemented in FPGA technology, wherein the layout is programmed in the FPGA circuitry either in a

volatile or non-volatile manner.

8. Method for manufacturing a secure device⁽¹¹⁾ for a security system according to anyone of claims 1-5 or for a set of secure devices⁽¹¹⁾ according to claim 6 or 7, wherein
5 secure devices⁽¹¹⁾ with a chip are used, said chips having logic circuitry having a function in providing authorization to the security system, wherein in at least ~~a part~~^{groups} of said secure devices, the chip of a secure device is ~~provided~~^{manufactured} with a unique chip layout.

10 9. Method according to claim 8, wherein chips with logic circuitry in FPGA technology are use, said method comprising the steps of programming a unique information⁽¹³⁾ in the logic circuitry by means of synthesis tool⁽²⁰⁾ and a layout tool⁽²²⁾, wherein for each secure device⁽¹¹⁾ of said part of secure
15 devices⁽¹¹⁾, a variation factor is introduced in at least one of the synthesis tool⁽²⁰⁾ and the layout tool⁽²²⁾, thereby providing a unique circuit layout.

10. Method according to claim 9, wherein the synthesis tool⁽²⁰⁾ is provided with input information compiled
20 from a high level language code^(17,18), wherein a variation factor⁽¹⁷⁾ is introduced in at least one of the compilation step of the high level language code^(17,18), the synthesis tool⁽²⁰⁾ and the layout tool⁽²²⁾.

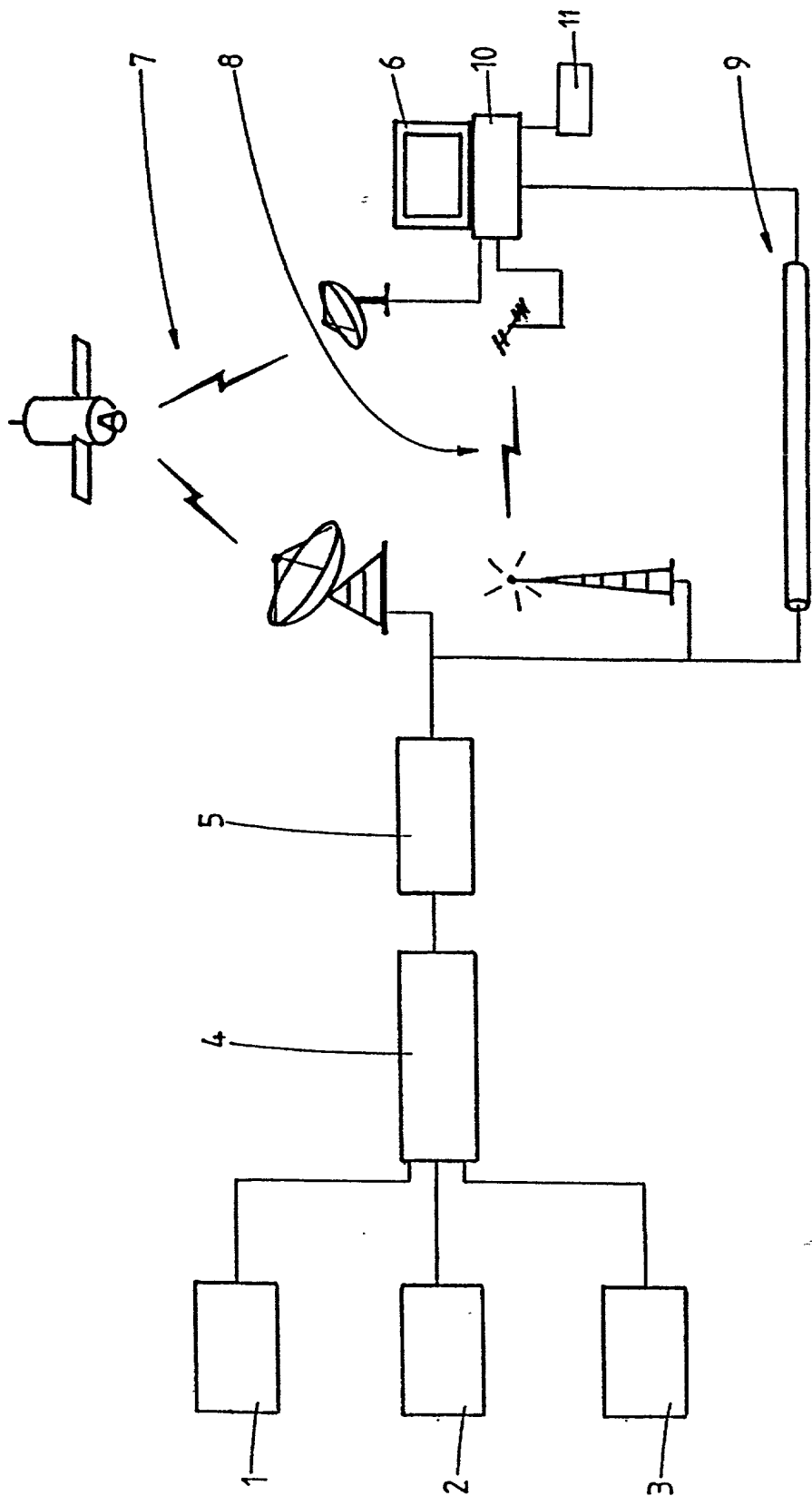


fig.1

09/763877

fig. 2

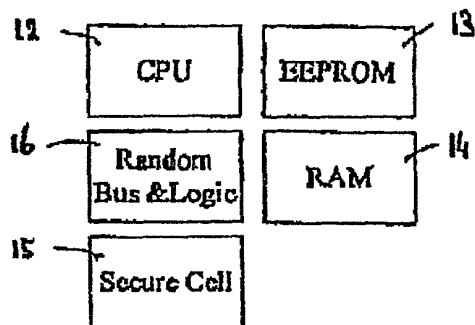
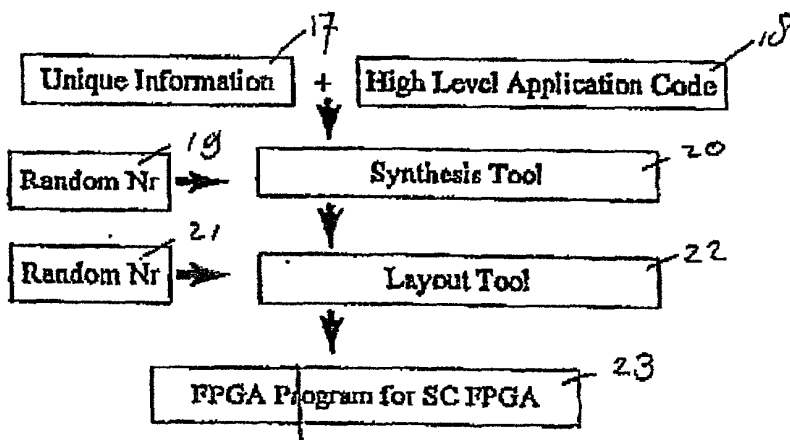


fig. 3



Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought, on the invention entitled **SECURITY SYSTEM**, the specification of which is attached hereto as Attorney Docket No. 82032-00006. ✓

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

			Priority Claimed	
<u>98202915.9</u> ✓	<u>EP</u> ✓	<u>01/September/1998</u> ✓	<input checked="" type="checkbox"/> [X]	<input type="checkbox"/> []
(Number)	(Country)	(Day/Month/Year)	Yes	No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

<u>(Application Serial No.)</u>	<u>(Filing Date)</u>
---------------------------------	----------------------

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the

manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/EP99/06340 — 30/August/1999 —
(Application Serial No.) (Filing Date) (Status)

I or we hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed to HOGAN & HARTSON, L.L.P., 555 13th Street, N.W., Washington, D.C. 20004, Customer No. 24633

Celine Jimenez Crowson, Reg. No. 40,357
Kevin G. Shaw, Reg. No. 43,110

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

FIRST NAMED INVENTOR	SIGNATURE	DATE
<u>Andrew Augustine WAJS</u>	<i>AA Wajs</i>	<u>2/2/2001</u>
RESIDENCE	CITIZENSHIP	
<u>NL-2023 AA Haarlem</u>	<u>GBN</u>	Great Britain
POST OFFICE ADDRESS		
<u>Schotersingel 93, NL-2023 AA Haarlem, The Netherlands</u>		